

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with easybit2222@gmail.com and
taltolit50@gmail.com, (the "accounts"), stored at premises
owned, maintained, controlled, or operated by Google LLC, as
further described in Attachment A

)
)
)
)
)
)
)

Case No. 23-969M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 10, 2023 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.

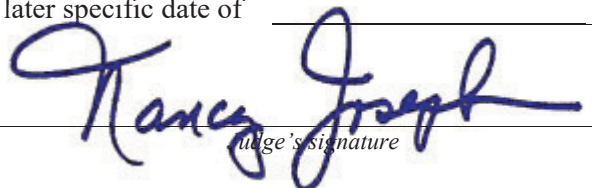
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____

Hon. Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 7/27/2023 @ 1:45 p.m.


Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **easybit2222@gmail.com** and **taltolit50@gmail.com**, (the “accounts”), that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Attachment B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government for each account or identifier listed in Attachment A the following information from September 1, 2017 to present, unless otherwise indicated:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;
- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity, including: search terms; browsing history, including application usage; bookmarks; passwords;

autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;
- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery

numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;
- **YOUTUBE WATCH HISTORY:** A record of the account's watch history, including: accessed URLs and their associated duration, privacy settings, upload timestamps, tags, IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history;
- **YOUTUBE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on YouTube, including birthday; name; username and other identifiers; linked accounts; alternate or recovery emails; telephone numbers, including SMS recovery numbers; physical addresses; account status; account creation date; account registration IP address; length of service; means and source of payment (including any credit or bank account number); associated devices; associated Android IDs; and associated logs and change history;

AdSense and AdWords

- **ADWORDS/GOOGLE ADS:** All records for advertising transactions by the account relating to Google Ads, AdWords, and DoubleClick for Advertisers, including: bid, location of advertisement (including URL), permitted advertisements, blocked advertisements, design and customization settings, and engagement records; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;
- **ADVERTISING SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on AdSense, Google Ads, Adwords, and DoubleClick by Google, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated

devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Connected Applications and Accounts

- **LINKED NON-GOOGLE ACCOUNTS:** All records relating to connected applications and websites not controlled by Google, including: applications and websites connected to the account at any time; associated account identifiers; privacy settings and account access permissions; and all associated logs, including access logs using Google credentials, timestamps, IP addresses, and change history;

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 641 (Theft of Government Property) since February 10, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Associated code and digital artifacts related to the creation of smart contracts;
- b. Identifying, hosting, maintaining, and registering domains and other means of online infrastructure;
- c. Registering websites, hosting websites, advertising, and client contact;
- d. Fraud or phishing;
- e. Finances, including cryptocurrency;
- f. The identity of the person(s) who created or used the Google ID; including records that help reveal the whereabouts of such person(s);
- g. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- h. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- i. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation, including interests and motivations; and

- j. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with easybit2222@gmail.com and
taltolit50@gmail.com, (the "accounts"), stored at premises owned,
maintained, controlled, or operated by Google LLC, as further described
in Attachment A

Case No. 23-969M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 1343 & 641	Wire fraud. Theft of government property.

The application is based on these facts:

See Attached Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Nicholas Johnson, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 7/27/2023

City and state: Milwaukee, WI

Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nicholas Johnson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google LLC (“Google”) to disclose to the government records and other information, including the contents of communications, associated with the Google accounts listed in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since December 2022. I am currently assigned to the FBI Milwaukee Division’s Cyber Crime Task Force. Prior to joining the FBI, I worked cyber operations within the private and public sectors. As a Special Agent with the FBI, I investigate criminal and national security-related computer intrusion matters involving cyber network exploitation, botnets, distributed denial of service attacks, malicious software, and the theft of personal identifiable information. Since joining the FBI, I have been involved in criminal and national security investigations involving computer intrusions. I have received education and training in cyber operations, threat hunting, and computer technology, and I have held industry certifications from GIAC and Microsoft.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of violations 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 641 (Theft of Government Property) as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. Since approximately 2020, the Drug Enforcement Administration (DEA), Milwaukee District Office (MDO) has been conducting a large-scale international money laundering investigation involving the use of cryptocurrency as a means to launder suspected drug proceeds. As a result of this investigation, on April 28, 2023, DEA case agents identified and froze two Binance cryptocurrency accounts involved in suspected money laundering. On May 5, 2023, DEA Special Agent (SA) Kellen Williams applied for and received a federal seizure warrant in the Eastern District of Wisconsin to seize Binance Account #197016535 (456,985.86843 USDT, DEA Exhibit N-320, Asset ID 23-DEA-703794) and Binance Account #27815331 (55,265.987213 USDT, DEA Exhibit N-321, Asset ID 23-DEA-703798). On June 6, 2023, Binance transferred a test sum of 45.36 USDT to a DEA-controlled Trezor cold storage

wallet. On June 15, 2023, Binance transferred the remaining 456,940.50843 cryptocurrency to the Trezor cold storage wallet for Exhibit N-320. Also on June 6, 2023, Binance transferred a test sum of 45.36 USDT to the Trezor cold storage wallet controlled by DEA agents. On June 15, 2023, Binance transferred the remaining 55,220.627213 cryptocurrency to the Trezor cold storage wallet for Exhibit N-321. On June 15, 2023, DEA agents verified the USDT transfers and transferred custody of the Trezor cold storage wallet to the DEA High Value Evidence Custodian for temporary storage.

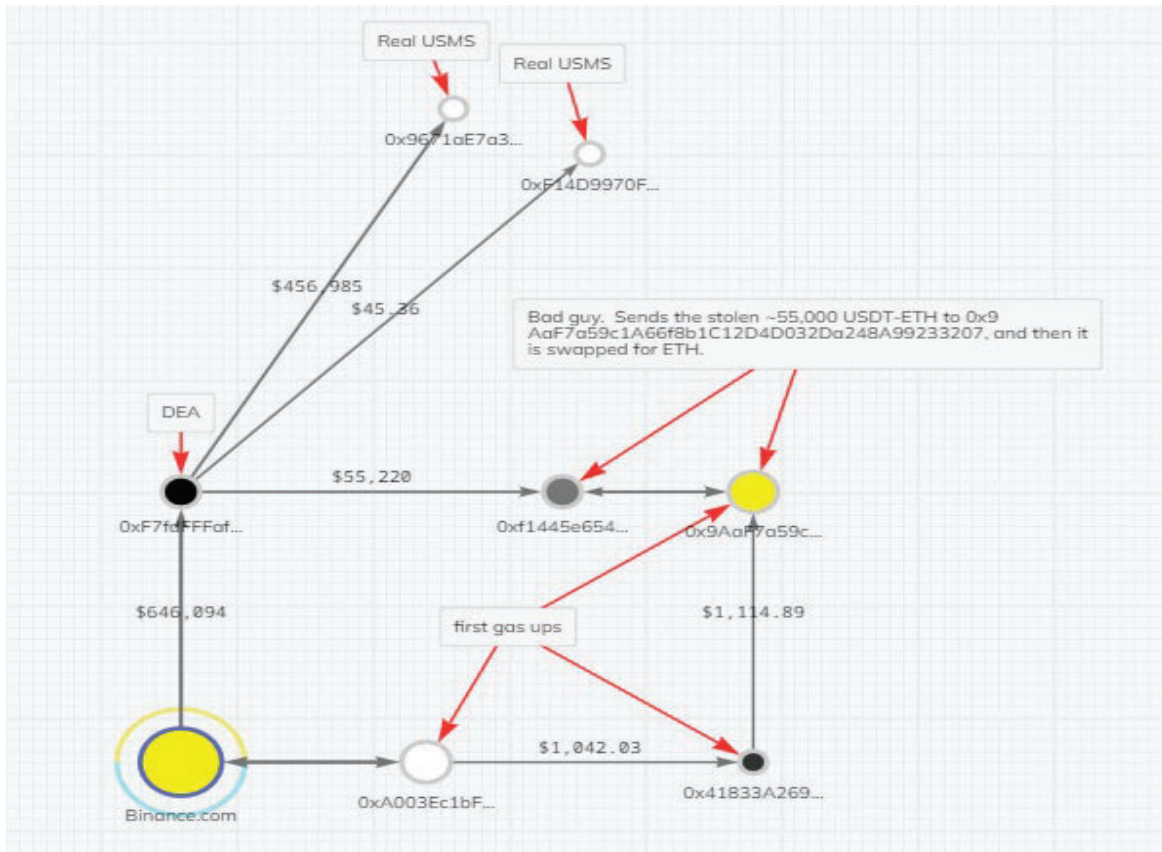
7. On June 20, 2023, DEA agents requested transfer of the virtual currency to the United States Marshals Service (USMS) for forfeiture processing. On July 7, 2023, the USMS approved the transfer. On this same date, DEA agents retrieved the Trezor cold storage wallet from the DEA High Value Evidence Custodian. DEA agents sent two test amounts of 45.36 USDT to the USMS provided wallet addresses, 0x9671aE7a32A2Bb4aFFaFB7c4713c60F994689a7e and 0xF14D9970FB2B9C750a87D1cbCD53dE0C942AB463 respectively. DEA agents contacted the USMS and verified receipt of the test transactions. Approximately 48 seconds after conducting the test transactions, and without the DEA agent's knowledge, two spoof USDT transactions appeared in the Trezor cold storage wallet transaction history mirroring the test transactions. Later investigation revealed that on July 16, 2023, (while the Trezor cold storage device was in DEA High Value Storage), the account was "airdropped" a spoofing scam. In summary, an attacker creates a "personal address" that can be configured with a certain set of characters, thereby it becomes similar to the address of the intended recipient. In this case, the spoof USDT transactions appeared to show a transfer of 45.36 USDT to wallet address 0xf1445e654AEdB88f75fCC56CBC4f47a9d685B463. The attacker created

0xf1445e654AEdB88f75fCC56CBC4f47a9d685B463 to mimic the USMS account of 0xF14D9970FB2B9C750a87D1cbCD53dE0C942AB463 in that the first 5 characters and the last 4 characters mimic the real wallet address.

8. Next, DEA agents sent the remaining balance of Exhibit N-320 (456,940.50843 USDT) to the correct USMS wallet address 0x9671aE7a32A2Bb4aFFaFB7c4713c60F994689a7e. DEA agents then proceeded to send the remaining balance of Exhibit N-321 (55,220.627213 USDT) to the USMS. Because the test transaction was successful, DEA agents went to the transaction history to copy the wallet address and mistakenly copied the spoof transaction address of 0xf1445e654AEdB88f75fCC56CBC4f47a9d685B463 instead of the correct USMS wallet address 0xF14D9970FB2B9C750a87D1cbCD53dE0C942AB463. After sending the funds to the attacker's address, DEA agents were immediately contacted by USMS and notified of the fraudulent activity.

9. DEA agents analyzed attacker address 0xf1445e654AEdB88f75fCC56CBC4f47a9d685B463 and found the 55,220.627213 USDT in the wallet. Working with the U.S. Attorney's Office in the Eastern District of Wisconsin, DEA agents sent a freeze letter on July 7, 2023, to Tether for the aforementioned 55,220.627213 USDT. On July 9, 2023, Tether responded that the funds have already been depleted and no longer able to freeze. Also on July 9, 2023, DEA agents, with the assistance of the FBI Virtual Asset Unit, analyzed the transactions and found the 55,220.627213 USDT was sent on July 8, 2023, to 0x9AaF7a59c1A66f8b1C12D4D032Da248A99233207 ("0x9Aa...33207"), where it was converted to ETH and remains in the wallet.

10. During additional review of the transactions, DEA agents located two Binance accounts which funded “gas fees” for 0x9Aa...33207 in 2021. On July 10, 2023, DEA agents issued an administrative subpoena to Binance, requesting account information for the two Binance accounts. On that same day, Binance responded to the subpoena and provided account information related to Binance User ID 36830321 and 78466101. Binance User ID 36830321 is registered to email account **easybit2222@gmail.com** and was created on May 18, 2019, and provided no Know Your Customer (“KYC”) information. A review of the access logs revealed the account is primarily logged into using IP addresses from Beersheba, Israel, Tel Aviv, Israel, Tiberias, Israel, Bnei Brak, Israel and Amsterdam, Netherlands. A review of the transactions revealed that the account has sent approximately 30.5111452 ETH to wallet address 0xA003Ec1bF50118D703ecA2f213aB474033aC6A72 (“0xA00...C6A72”). On June 20, 2023, 0xA00...C6A72 sent 0.60 ETH to 0x41833A2698A331b7bfBC461cdf0a13c0D059DE9c. On June 27, 2023, 0x418...9DE9c sent 0.599666 ETH as “gas fees” to 0x9Aa...33207.



11. Binance User ID 78466101 is registered to email account **taltolit50@gmail.com** and was created on February 10, 2021, and provided no KYC information. A review of the access logs revealed the account is primarily logged into using IP addresses from Petah Tikva, Israel, Tel Aviv, Israel, Tiberias, Israel, and Kyiv, Ukraine. A review of the transactions revealed that the account has sent approximately 1.01549723 ETH and 84,000 USDT to wallet address 0xA003Ec1bF50118D703ecA2f213aB474033aC6A72 (“0xA00...C6A72”), mentioned above.

12. During a review of IP address from both Binance User IDs 36830321 and 78466101, case agents believe Binance User ID 36830321 utilizes a VPN masking the IP address to appear to come from the Netherlands. However, on multiple occasions in 2021, Binance User IDs 36830321 and 78466101 log into their respective accounts using the exact same IP address

on the same day. Based on their training and experience, case agents believe Binance User IDs 36830321 and 78466101 are controlled by the same person. As a result, based on their training and experience, case agents believe **easybit2222@gmail.com** and **taltolit50@gmail.com** are controlled by the same person.

13. A search of social media revealed a Facebook account under user ID tal.aviv.5 associated with the email **taltolit50@gmail.com**. A review of old posts under that account identified posts where the user of that Facebook account directed people to email **taltolit50@walla.com**. A review of the friends list under tal.aviv.5 revealed "Daniel" under Facebook user account daniel.barchiel.

14. Based on my training and experience as well as my knowledge and information garnered from other similar cases, I know that individuals who engage in the laundering of stolen cryptocurrency funds will communicate and send and receive information through electronic communication such as e-mails and chats. In this investigation, case agents are aware that the two Binance accounts are involved in cryptocurrency transactions and would likely receive email confirmation of these transactions in the **easybit2222@gmail.com** and **taltolit50@gmail.com** accounts. Furthermore, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

15. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

16. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND CONCERNING GOOGLE

17. Google is a United States Company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome and a free search engine called Google Search.

18. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device.

19. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. Enterprises may also establish Google Accounts which can be accessed using an email address at the enterprise's domain (e.g., employee[@]company.com).

20. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, some of which are described in further detail below. In addition, Google

keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

21. **GMAIL:** Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses (“recovery,” “secondary,” “forwarding,” or “alternate” email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

22. **CONTACTS:** Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their mobile phone or device address book, so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them.

23. **CALENDAR:** Google provides an appointment book for Google Accounts through Google Calendar. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device

address book, so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them.

24. **GOOGLE KEEP:** Google also provides online to-do lists and notepads for Google Accounts. Google Keep allows users to create notes or lists. These notes can be shared with other users to edit. Users can set notifications at particular dates and times for both tasks and notes. Google preserves tasks and notes indefinitely, unless the user deletes them.

25. **WEB-BASED CHATS and MOBILE MESSAGING:** Google provides a number of direct messaging services accessible through a browser or mobile application, including Duo, Messages, Hangouts (Chat and Meet), and the now-retired Allo and Chat. These services enable real-time communications. Users can send and receive text messages, videos, photos, locations, links, and contacts from their Google Account using these services. Chat and Hangouts require or required the other user to also have a Google Account. Duo, Messages, and Allo do or did not. Google preserves messages sent through these services indefinitely, unless the user turns off the setting to save conversation history or deletes the message.

26. **GOOGLE DRIVE:** Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can also set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows

users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called “Shared with me.” Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

27. **GOOGLE DRIVE FOR ANDROID USERS:** Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, and file downloads. If a user subscribes to Google’s cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

28. **GOOGLE PHOTOS:** Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

29. **GOOGLE MAPS and GOOGLE TRIPS:** Google offers a map service called Google Maps that can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can

save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

30. **GOOGLE PLAY:** Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

31. **GOOGLE VOICE:** Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

32. **GOOGLE CHROME:** Google offers a free web browser service called Google Chrome that facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account.

33. **YOUTUBE:** Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than

one user can share control of a YouTube channel. YouTube may keep track of a user's searches, watch history, likes, comments, and change history to posted videos.

34. **INTEGRATION OF GOOGLE SERVICES:** Google integrates these various services to make it easier for Google Accounts to access the full Google suite of services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

Google Account Records:

35. **SUBSCRIBER RECORDS:** When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

36. **ACCESS RECORDS:** Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account

(including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

37. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

38. **BROWSING, SEARCH, and APPLICATION USE HISTORY:** Google collects and retains data about searches that users conduct within their own Google Account or using the Google Search service, including voice queries made to Google Assistant. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google also collects and retains data about the voice queries made to its artificial intelligence-powered virtual assistant, Google Assistant, on Android devices and associated it with the registered Google Account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google usually maintains these records indefinitely, unless the user deletes them.

39. **LOCATION HISTORY:** Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices, regardless of service usage. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Google maintains these records indefinitely unless the user deletes it or [not yet implemented: opts into automatic deletion of their location history every three or eighteen months].

40. **ANDROID DEVICE DATA:** When an individual uses an Android device for the first time, they are prompted to register the device to a new or existing Google Account. Data about the use of the Android device is saved to the registered Google Account, including device characteristics such as the device serial number, model type/number, and international mobile equipment identity (IMEI). In addition, users may opt-in to Android device backups to Google cloud servers. Android device backups are only saved as a unique backup file if the user subscribes to Google's cloud storage service, Google One. If they do not, data from the device is associated with the registered Google Account and stored with similar data in the Google Account. For example, photos and videos on the device are backed up to Google Photos;

contacts are backed up to Google Contacts; events and appointments are backed up to Google Calendar; and files and certain application data are backed up to Google Drive. Google maintains these records indefinitely, though users may delete Android back-up files in the same manner as any other file associated with the relevant Google service.

41. Google also maintains records of the device characteristics of iPhones used to access Google services, including the make and model of the device. Depending on user settings, those records may be associated with the Google Account logged into the service in use on the device. Google maintains these records indefinitely, unless the user deletes them.

42. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, where, when, why, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

43. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

44. In addition, the user’s account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy”

while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

45. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

46. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, location information, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

47. As noted herein, the actors behind the aforementioned smart contract is continuing to perpetrate fraud. The Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my

training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

48. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

49. Based on the forgoing, I request that the Court issue the proposed search warrant.

50. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **easybit2222@gmail.com** and **taltolit50@gmail.com**, (the “accounts”), that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Attachment B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government for each account or identifier listed in Attachment A the following information from September 1, 2017 to present, unless otherwise indicated:

Google Account

- **SUBSCRIBER AND ACCESS RECORDS:** All business records and subscriber information, in any form kept, pertaining to the account, including: full name; physical address; telephone numbers, including SMS recovery and alternate sign-in numbers; alternative and recovery email addresses, including those provided during registration; usernames, screennames and other identifiers; account status; account creation date; account registration IP address; length of service; records of session times and durations, including log-in IP addresses; methods of connecting; log files; subscriber change history; means and source of payment (including any credit or bank account number); and detailed billing records;
- **DEVICES:** All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- **SERVICES:** The types of services utilized, including connected applications and sites, and any dates associated with the commencement or termination of that use;
- **FORWARDING OR FETCHING ACCOUNTS:** All forwarding or fetching accounts relating to the accounts;
- **BROWSING, SEARCH, and APPLICATION USE HISTORY:** All Internet search, browsing history, and application usage history, such as Web & App Activity, including: search terms; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including

associated notifications and creation dates; all text typed into the Google Chrome address bar or Google search bar, including URLs and IP addresses; all URLs or IP addresses clicked on; user settings; and all associated logs and change history;

- **LOCATION HISTORY:** All records indicating the location at which the account was active, such as Location History and Web & App Activity, including: GPS data; cell site/cell tower information; IP addresses; information associated with each location record, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, and inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car); and associated logs and user settings, including Timeline access logs and change history;

Gmail

- **GMAIL:** The contents of all emails associated with the account, including, but not limited to: stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the date and time at which each email was sent; the size and length of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails;
- **CONTACTS:** Any records pertaining to the user's contacts, including: address books; contact lists, including autocomplete suggestions; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history;
- **CALENDAR:** Any records pertaining to the user's calendar, including: Google Calendar entries; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history;
- **WEB-BASED CHATS:** The contents of all chats associated with the account, including Google Hangouts, Meet, and Chat, in any format (text, audio, or video) including, but not limited to: stored, deleted, and draft chat communications, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size and length of each communication; user settings; and all associated logs, including access logs and change history;

Google Drive

- The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes, lists,

applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Photos

- The contents of all media associated with the account in Google Photos or Picasa, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; third-party data; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs, including access logs and IP addresses, of each record;

Google Maps and Trips

- All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; information associated with locations and other data associated with My Maps and Location Sharing; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history;

Google Play Store

- All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, movies, music, television shows, books, magazines, games, and other files; details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;

Messaging Services

- **MOBILE MESSAGING:** The contents of all messages associated with the account, including Google Duo, Android Messages, and Google Allo, in any format (e.g. SMS, MMS, or RCS) including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses and telephone numbers; the size and length of each communication; associated telephone numbers, including SMS recovery

numbers; usernames and other identifiers; user settings; and all associated logs and change history;

YouTube

- **YOUTUBE CONTENTS:** The contents of all media associated with the account on YouTube, whether active, deleted, or in draft, including: copies of videos and other media only if uploaded to, saved to, shared by or shared with the account; edits, comments, likes, chats, and other interactions, including associated URLs; search history; channels; subscriptions; subscribers, friends, and other contacts; playlists; connected applications; associated URLs for each record; creation and change history; privacy settings for each record; and all associated logs, including IP addresses, locations, timestamps, and device identifiers;
- **YOUTUBE WATCH HISTORY:** A record of the account's watch history, including: accessed URLs and their associated duration, privacy settings, upload timestamps, tags, IP addresses, change history, location information, and uploading account or identifier; the logs for each access by the account, including IP address, location, timestamp, and device identifier; and change history;
- **YOUTUBE SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on YouTube, including birthday; name; username and other identifiers; linked accounts; alternate or recovery emails; telephone numbers, including SMS recovery numbers; physical addresses; account status; account creation date; account registration IP address; length of service; means and source of payment (including any credit or bank account number); associated devices; associated Android IDs; and associated logs and change history;

AdSense and AdWords

- **ADWORDS/GOOGLE ADS:** All records for advertising transactions by the account relating to Google Ads, AdWords, and DoubleClick for Advertisers, including: bid, location of advertisement (including URL), permitted advertisements, blocked advertisements, design and customization settings, and engagement records; payment transactions; user settings; and all associated logs, including IP addresses, location data, timestamps, and change history;
- **ADVERTISING SUBSCRIBER RECORDS:** All business and subscriber records associated with the account on AdSense, Google Ads, Adwords, and DoubleClick by Google, including: name; user name; physical address; alternate or recovery emails; telephone numbers, including SMS recovery numbers; linked accounts; account status; account creation date; account registration IP address; length of service; associated

devices; associated AndroidIDs; means and source of payment (including any credit or bank account number); and all associated logs and change history;

Connected Applications and Accounts

- **LINKED NON-GOOGLE ACCOUNTS:** All records relating to connected applications and websites not controlled by Google, including: applications and websites connected to the account at any time; associated account identifiers; privacy settings and account access permissions; and all associated logs, including access logs using Google credentials, timestamps, IP addresses, and change history;

The Provider is hereby ordered to disclose the above information to the Government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 641 (Theft of Government Property) since February 10, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Associated code and digital artifacts related to the creation of smart contracts;
- b. Identifying, hosting, maintaining, and registering domains and other means of online infrastructure;
- c. Registering websites, hosting websites, advertising, and client contact;
- d. Fraud or phishing;
- e. Finances, including cryptocurrency;
- f. The identity of the person(s) who created or used the Google ID; including records that help reveal the whereabouts of such person(s);
- g. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- h. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- i. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation, including interests and motivations; and

- j. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.